PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/32, 7/22

A2

(11) International Publication Number: **WO 98/27768**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/GB97/03440

(22) International Filing Date: 15 December 1997 (15.12.97)

(30) Priority Data:
9626030.2 14 December 1996 (14.12.96) GB

(71) Applicant *(for all designated States except US)*: CENTRAL RESEARCH LABORATORIES LIMITED [GB/GB]; Dawley Road, Hayes, Middlesex UB3 1HH (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SIBBALD, Alastair [GB/GB]; 18 Horseguards Drive, Maidenhead, Berkshire SL6 1XL (GB). TODD, Martin, Peter [GB/GB]; 17 Honeycroft Hill, Uxbridge, Middlesex UB10 9NQ (GB).

(74) Agent: LEAMAN, Keith; QED Patents Limited, Dawley Road, Hayes, Middlesex UB3 1HH (GB).

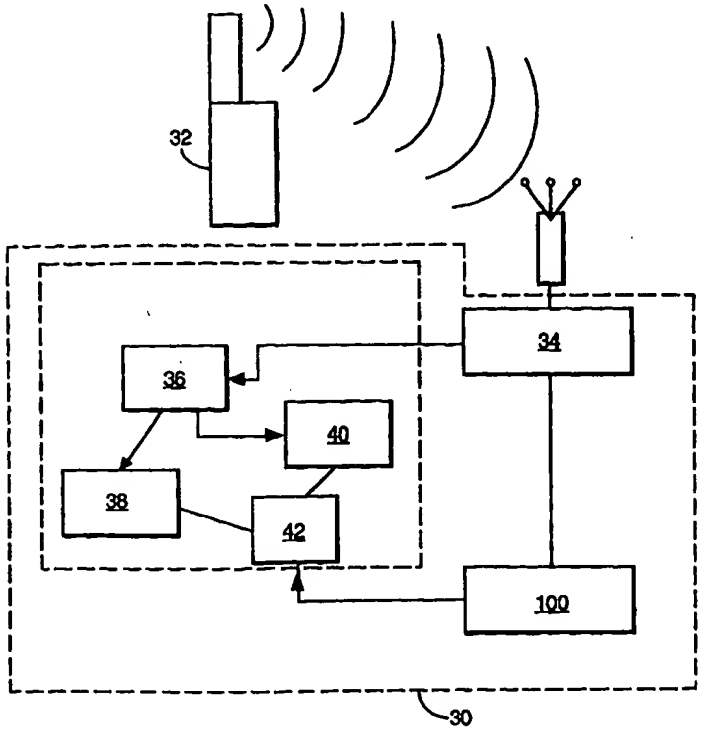
(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: MOBILE TELEPHONE SECURITY

(57) Abstract

The invention is a method of making a mobile telephone more secure and includes generating an identification code, inserting the code into transmitted speech, detecting the code at a base station and comparing it with stored information to verify the authenticity of the mobile telephone. The identification code comprises two portions: the first portion (which stores the code) being produced during manufacture of a chip and the second portion being formed by a randomised process during commissioning of the telephone. The invention overcomes problems associated with similar, prior art systems because the chip containing the identification code has part of its code randomly selected because it is an irreversible process.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Paso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Mobile Telephone Security

The present invention relates to a means of making a mobile telephone more secure against counterfeiting, otherwise know as cloning.

Such counterfeiting occurs when a genuine mobile telephone signal is intercepted by a counterfeiter (scanned) and the security code (telephone or account number and electronic serial number of the actual handset) of the genuine telephone is recorded. This code is then used to re-program a stolen mobile telephone, thus producing a counterfeit of the genuine mobile telephone which can be used to make calls which will be billed to the genuine telephone's account. The cloning of mobile telephones is currently limited to analogue networks. It represents a very large proportion of telephone calls made. One recent estimate (New Scientist 9 Nov 96 pp.20) is £200 million per year in the U.K. alone. Much of this illegal traffic (particularly in the U.S.A.) is crime related, and the calls are often international. The major aspect of the problem is not the stolen telephones which might be reported and cancelled by the network, but the aspect whereby a legitimate telephone is still in operation with its owner not aware of any problem, and a clone is running up a bill on the same telephone. Thus any solution must either make it difficult to clone, or must detect a clone in operation. A solution which would allow the genuine telephone to continue operating would be of benefit. Any solution must be cheap in terms of any additional cost to the handset. The handsets are often sold at, or below, cost. Any solution should have minimal impact on the existing network base stations in terms of re-engineering, and again minimal cost.

There are existing methods by which the cloning of a telephone can be detected.

1) A change in calling pattern. This is probably the only method in general use.

The network providers can detect when the calling pattern of a particular telephone changes and check with the owner that the calls being made are genuine.

2) The RF footprint of every telephone. Each individual telephone has a slightly different RF response, and the RF footprints can be recorded at the base station as a call comes in. The footprint is then compared to the database for that account.

There is a system available for this, but currently costing around £100,000 per base station, it is considered too expensive.

UK Patent Application Nos GB-A-2163323 and EP-A-6167331 describes signal transmission systems for telecommunication equipment. In both systems code is insterted into a transmitted signal. However, the encoder and technique is relatively complex.

Summary of the Invention

The present invention provides a method of making a mobile telephone handset more secure comprising:

1) Providing in a handset a means for generating at periodic intervals an identification code;

2) When the handset is being used to transmit speech, inserting said identification code into the speech signal in such a way that the identification code cannot be heard;

3) Providing in a base station a means for recognising said code in said speech patterns, the base station comparing the received code information with recorded information to identify the transmitting handset.

In a further aspect, the present invention provides a mobile telephone handset including means for generating an identification code at predetermined intervals, and means for inserting said identification code into transmitted speech signals in such a way that the code is inaudible.

The use of transmitted identification codes in broadcast signals for commercial radio stations and television stations is described in our granted European Patent EP-B-0245037 and published International Patent Application WO-A-9621290. EP-B-0245037 discloses apparatus for labelling an audio signal comprising filters to eliminate a plurality of frequency notches from an audio signal, code generating means to produce a code signal having an identifying portion and a message portion represented by bursts of frequencies at the notch frequencies, and inserting the frequency bursts into the

notches in the audio signal. Monitoring means is provided to monitor the amplitude of the audio signal and to ensure that the inserted code signals have an amplitude relative to that of the audio signal so that they will not normally be heard.

Preferably the present invention provides each handset of a telephone with an encoder chip which is connected in the audio path, and is arranged into encode identification (ID) code containing a single serial number audio signals in real-time before the signals are transmitted,

A database is maintained of the ID codes which correspond to each account number (teletelephone number).

A plurality and preferably all base-stations contain one or more decoder chips which decode incoming signals for their ID codes.

If the decoded ID code matches the data base number, then the call is valid. If not, the call is considered counterfeit and dealt with in a manner to be determined by the network operator. The options can include disconnection, feeding a signal back to "lock" the handset, and logging the number called for the authorities to investigate.

To circumvent the invention, the counterfeiter would need to read the ID code from a genuine telephone and clone it in the stolen telephone. This would be quite difficult for the following reasons.

1. Encoder chips are blown with a random serial number at manufacture (perhaps during testing). This involves an irreversible process, for example burning-out resistors. The serial number is sufficiently large to prevent a counterfeiter from having a full set of chips to select from. The pre-blown chips are held securely to ensure they are not stolen. To allow for this possibility, some of the ID code is hard-wired by the chip mask, and if a serious security breach is detected the mask is altered, and codes with the known hard-wired code not used. However, even if stolen, the chip has a random

process within it for blowing the number, making it difficult for the counterfeiter to blow a particular desired number.

2. To read the ID code off-air, the counterfeiter would need a more sophisticated scanner which incorporates a decoder.

3. Since the encoder chip is not reprogrammable, the counterfeiter would have to replace it by a chip with the same function. By making the encoding process sufficiently complex, this would require a Digital Signal Processor (DSP) or other complex processor to perform the operation. By building in detection circuitry, which analyses current and voltages, it is made difficult for the counterfeiter to insert such programmable devices into the telephone itself. An alternative would be to cut PCB tracks within the telephone and attach a PC or "black box" into the circuitry. This would be bulky and need to remain attached whilst in use. Alternatively the counterfeiter would have to make a re-programmable chip. All these "work-arounds" make it more expensive for the counterfeiter to clone each telephone, and will make a cloning operation more difficult. This willcut out all but the most serious of counterfeiters.

Brief Description of the Drawings

A preferred embodiment of the invention will now be described with reference to the accompanying drawings wherein:-

Figure 1 is a schematic view of an encoder chip for use in a mobile teletelephone handset;

Figure 2 is a block diagram of the internal construction of the chip; and

Figure 3 is a schematic system diagram showing a mobile teletelephone handset in connection with a base station employing a decoding mechanism in accordance with the invention.

Description of the Preferred Embodiment

Referring now to Figure 1, the encoder chip has a simple 6 pin structure and a relatively low power consumption. Pin 1 provides an audio input for speech to be transmitted, pin 2 provides an audio output, pin 3 is a ground, pin 4 is power, pin 5 is an erase signal and pin 6 receives a clock signal. Pin 5 is employed to blow an ID serial number into the chip.

Referring to Figure 2, the encoder chip comprises notch filter 10 for removing two narrow bands at selected notch frequencies from an incoming signal. A coding unit 12 assesses the audio signal strength and provides alternate frequency bursts at the two notch frequencies to represent an ID code stored in a store 14. These frequency bursts are inserted into the audio signal output from notch filters 10 in a combining unit 16 to provide an audio output on line 16. Details of units 10, 12, 14 are given in EP-B-0245037 and WO-A-9621290.

Memory store 14 is divided into two parts, a first part 18 containing part of the ID serial number taken from the chip mask, and a second part 20 left blank, to be blown-in during testing, as is shown in the example format below. The exact length and split of this format may be varied. For the 36-bit data code suggested here, the ID process is likely to use an additional 16-20 bits for error correction overhead, giving a total 50-60 bit actual code. This improves the robustness of the scheme:-

16-bit (65536 masks) - 20-bit (1048576 possible codes)

XXXXXXXXXXXXXXXX - XXXXXXXXXXXXXXXXXXXX

samples from the same batch:-

13568 - 0219203

13568 - 1006255

13568 - 0563750

The fact that two chips may by chance have the same ID serial number does not matter, since in the application of the chip it is the correlation between the account number and ID number that counts, not whether any two accounts have the same ID number. There is a chance that a stolen telephone has the same number as a genuine one being cloned; however, the chance of this is insignificant (one in a million for a particular mask).

Referring now to Figure 3, this shows a schematic block diagram of a base station 30 which receives signals transmitted from handset 32. A demultiplexor 34 separates the incoming signal from the other incoming signals and passes it to a splitter 36, which separates the account number code, which is normally present in the handset transmissions. The account number is used to access a database 38, which among other verification operations provides an ID serial number for the handset associated with the account number. At the same time, a decoder unit 40 coupled to splitter 36, analyses the speech signals and derives the ID serial code present in the notch frequencies, essentially by the inverse of the encoding process as described above. The two derived codes are compared in a comparator 42. If they correspond, no further action is necessary, but if they do not correspond, indicating a possible illegality, appropriate measures may be initiated as outlined above.

The decoding process is a process which analyses the incoming signal and reports the ID serial number. For the 50-60 bit actual code suggested above, it would be expected to take about 20 seconds to confirm the code in a reliable manner. The time taken to confirm the code will depend on the quality of the audio signal. Additionally, there is a trade-off which can be made by making the code more audible (and also to be present in silent periods), and so this time period can be reduced. Higher quality means shorter "time to confirm". If the counterfeiter tries to use this to circumvent the ID code, the system could detect that multiple short calls are being made to the same number with no ID confirmation.

The invention has been described by way of example only and variation may be made to the embodiment described.

CLAIMS

1. A method of making a mobile telephone handset more secure comprising:

i) providing in a handset a means for generating at periodic intervals an identification code;

ii) when the handset is being used to transmit speech, inserting said identification code into the speech signal in such a way that the identification code cannot be heard; and

iii) providing in a base station a means for recognising said code in said speech signal patterns, the base station comparing the received code information with record information to identify the transmitting handset, characterised in that the code is held in a memory store in two parts, a first part being formed during manufacture, and a second part being formed by a randomised process during handset commissioning.

2. A method according to claim 1, wherein the identification code is in the form of bursts at predetermined frequencies and is inserted into the speech signal where the audio signal has been filtered out at such frequencies.

3. A mobile telephone handset including means for generating an identification code at predetermined intervals, and means for inserting said identification code into transmitted speech signals in such a way that the code is inaudible.

4. A mobile telephone handset according to claim 3, wherein the code is held in a memory store in two parts, a first part being formed during manufacture, and the second part being formed by a randomised blowing means operative in response to an external control signal.

5. A base station including means for separating a coded signal transmitted from a telephone, into an audio data carrying portion and a portion containing coded information and means for comparing the coded information with stored information specific to said telephone.

Fig.1.

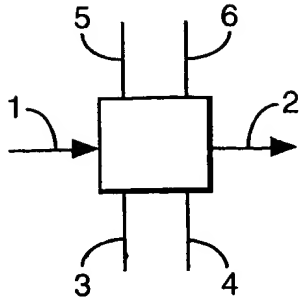


Fig.2.

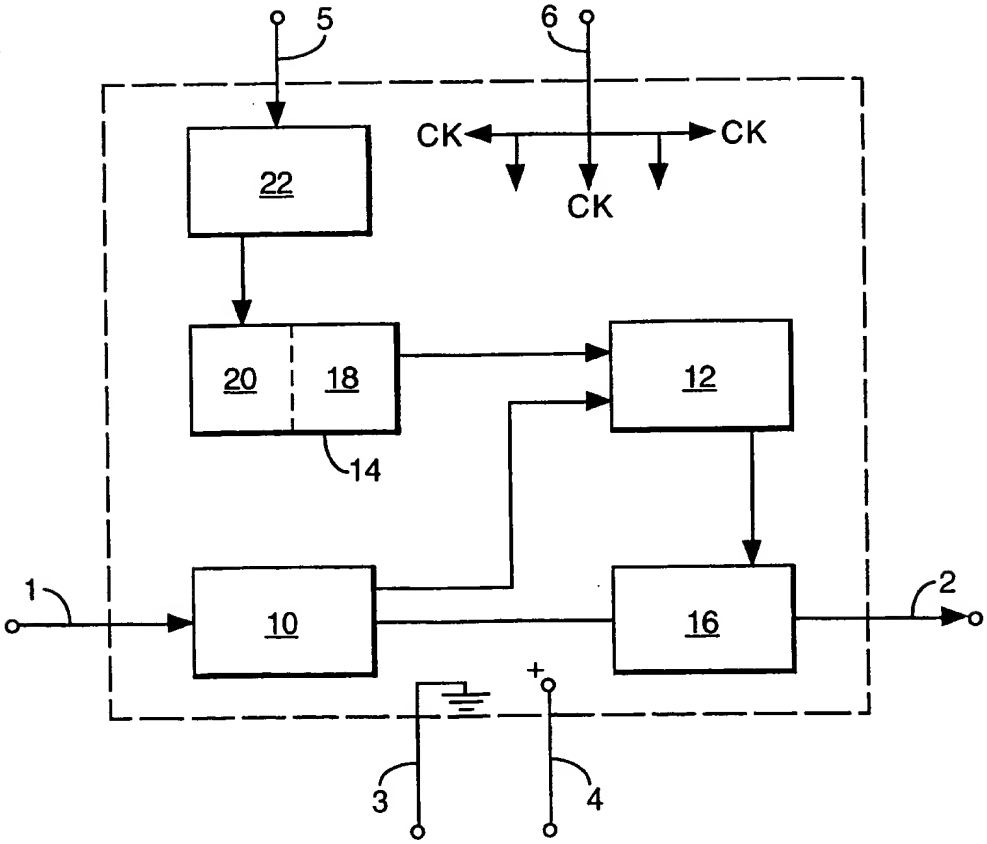
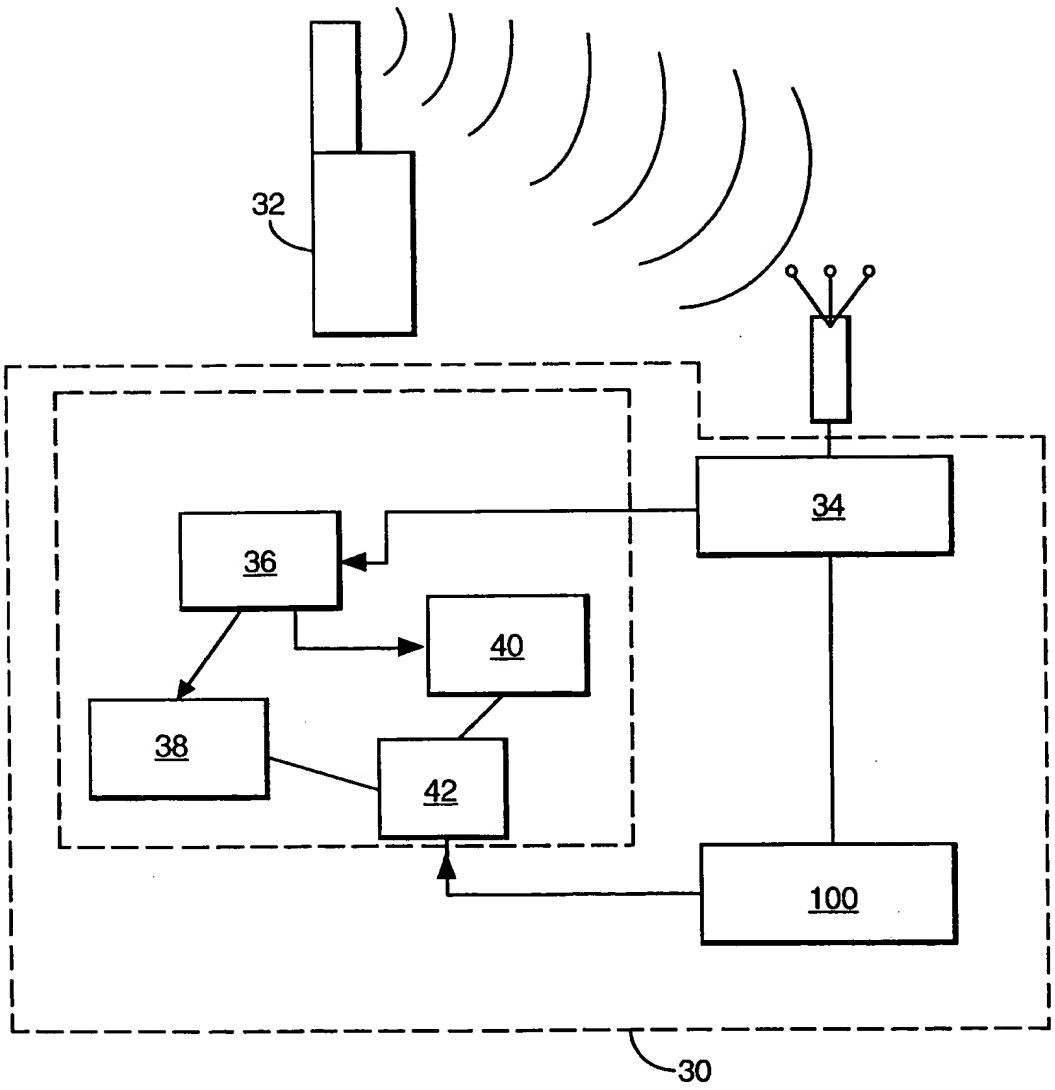


Fig.3.



PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/32, 7/38

A3

(11) International Publication Number: **WO 98/27768**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/GB97/03440

(22) International Filing Date: 15 December 1997 (15.12.97)

(30) Priority Data:
9626030.2 14 December 1996 (14.12.96) GB

(71) Applicant *(for all designated States except US)*: CENTRAL RESEARCH LABORATORIES LIMITED [GB/GB]; Dawley Road, Hayes, Middlesex UB3 1HH (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SIBBALD, Alastair [GB/GB]; 18 Horseguards Drive, Maidenhead, Berkshire SL6 1XL (GB). TODD, Martin, Peter [GB/GB]; 17 Honeycroft Hill, Uxbridge, Middlesex UB10 9NQ (GB).

(74) Agent: LEAMAN, Keith; QED Patents Limited, Dawley Road, Hayes, Middlesex UB3 1HH (GB).

(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

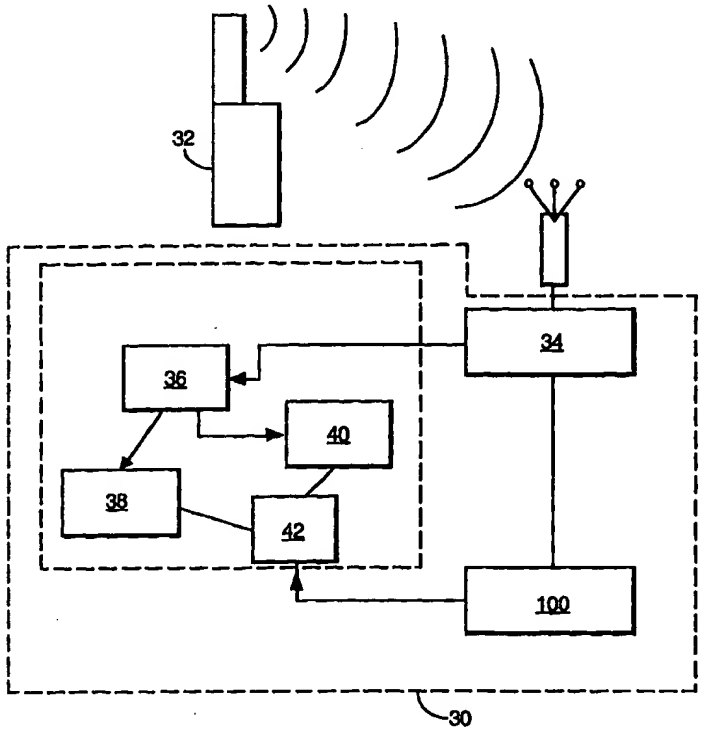
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
23 December 1998 (23.12.98)

(54) Title: MOBILE TELEPHONE SECURITY

(57) Abstract

The invention is a method of making a mobile telephone more secure and includes generating an identification code, inserting the code into transmitted speech, detecting the code at a base station and comparing it with stored information to verify the authenticity of the mobile telephone. The identification code comprises two portions: the first portion (which stores the code) being produced during manufacture of a chip and the second portion being formed by a randomised process during commissioning of the telephone. The invention overcomes problems associated with similar, prior art systems because the chip containing the identification code has part of its code randomly selected because it is an irreversible process.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 97/03440

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/32 H04Q7/38

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 167 331 A (SONY CORP) 8 January 1986 cited in the application	3
A	see abstract see page 3, line 19 - page 4, line 32 see page 8, line 8 - line 31 see page 9, line 33 - page 14, line 22 see figures 2A,2B,3-6 ---	1,2,4,5
A	GB 2 163 323 A (BRITISH TELECOMM) 19 February 1986 cited in the application see abstract see page 1, line 76 - line 119 see page 2, line 4 - line 107 see figures 1-3 --- -/--	1-5

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
1 September 1998	02/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cochonneau, O

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/GB 97/03440

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 21290 A (CENTRAL RESEARCH LAB LTD ;BEST STUART JOHN (GB); TODD MARTIN PETER) 11 July 1996 cited in the application see abstract see page 2, line 19 - page 4, line 24 see page 6, line 19 - page 9, line 16 see page 10, line 21 - line 30 see figures 3-6	1-3,5
A	US 5 392 356 A (KONNO MASAHIRO ET AL) 21 February 1995 see abstract see column 3, line 50 - column 4, line 60 see column 5, line 21 - column 6, line 37 see figures 1,2	1,4
A	WO 92 12584 A (MOTOROLA INC) 23 July 1992 see abstract see page 2, line 3 - line 32 see page 3, line 15 - page 6, line 25 see figures 1-4,4A	1,4
A	LO J: "WHO YA GONNA CALL?" TELEPHONY, vol. 229, no. 9, 28 August 1995, pages 22-24, 26, XP000617459 see page 24, column 2, line 62 - page 25, column 1, line 18	1,3,5
A	GB 1 498 283 A (TEKADE FELTEN & GUILLEAUME) 18 January 1978 see page 1, line 83 - page 2, line 41 see figures 1-3	1,3,5

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/GB 97/03440

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0167331 A	08-01-1986	JP 61009039 A	16-01-1986
		AU 585514 B	22-06-1989
		AU 4378985 A	02-01-1986
		CA 1235753 A	26-04-1988
		DE 3587027 A	11-03-1993
		US 4679225 A	07-07-1987
GB 2163323 A	19-02-1986	DE 3587716 D	17-02-1994
		DE 3587716 T	28-04-1994
		EP 0176215 A	02-04-1986
WO 9621290 A	11-07-1996	CA 2209621 A	11-07-1996
		EP 0801855 A	22-10-1997
US 5392356 A	21-02-1995	JP 6224843 A	12-08-1994
		GB 2274565 A,B	27-07-1994
WO 9212584 A	23-07-1992	US 5077790 A	31-12-1991
		AU 8769091 A	17-08-1992
		CA 2087841 A,C	01-07-1992
		EP 0565528 A	20-10-1993
		FI 930307 A	26-01-1993
		JP 2546756 B	23-10-1996
		JP 6505837 T	30-06-1994
		KR 9600935 B	15-01-1996
GB 1498283 A	18-01-1978	DE 2419615 A	06-11-1975
		CH 584495 A	31-01-1977
		FR 2269263 A	21-11-1975
		JP 1029720 C	22-01-1981
		JP 50145002 A	21-11-1975
		JP 55019537 B	27-05-1980
		NL 7504779 A	28-10-1975
		SE 398286 B	12-12-1977
		SE 7504695 A	27-10-1975